Validação de Simulações Quânticas

Verifying quantum computations

A. Rodrigues   L. Barbosa   C. Tavares

INESC TEC & Universidade do Minho

ARCA, 16 Mar 2018

2018-03-16

Validação de Simulações Quânticas

Validação de Simulações Quânticas
Verifying quantum computations

A. Rodrigues   L. Barbosa   C. Tavares

INESC TEC & Universidade do Minho

ARCA, 16 Mar 2018

Outline

Outline

1. Quantum Simulation
   - Motivation
   - Analog and digital quantum simulation
   - Assessing quantum simulators
2. Quantum Tomography
   - Quantum State Tomography
   - Quantum Process Tomography
3. Verifying high-complexity systems
   - Quantum interactive proofs
   - Blind quantum computation
4. Hands-on: IBM Q Network

Outline

Outline
1 Quantum Simulation
- Motivation
- Analog and digital quantum simulation
- Assessing quantum simulators
2 Quantum Tomography
- Quantum State Tomography
- Quantum Process Tomography
3 Verifying high-complexity systems
- Quantum interactive proofs
- Blind quantum computation
4 Hands-on: IBM Q Network

Quantum simulation

Why pursue quantum simulation?

- Classical representation of quantum states requires exponential resources
- The required number of gates scales exponentially as well

Quantum simulation
Why pursue quantum simulation?
- Classical representation of quantum states requires exponential resources
- The required number of gates scales exponentially as well

A descrição de sistemas quânticos utilizando computação clássica requer memória que escala exponencialmente com o número de elementos do sistema. Para mais, a evolução do sistema requer um número de operações que também escala exponencialmente com o tamanho do sistema ("explosão" exponencial não só em memória, como no tempo).

Outline

Outline

1. Quantum Simulation
   - Motivation
   - Analog and digital quantum simulation
   - Assessing quantum simulators
2. Quantum Tomography
   - Quantum State Tomography
   - Quantum Process Tomography
3. Verifying high-complexity systems
   - Quantum interactive proofs
   - Blind quantum computation
4. Hands-on: IBM Q Network

Uma simulação quântica genérica envolve a preparação de um estado inicial, a evolução temporal desse estado (Hamiltoneano) conforme especificações arbitrárias, e a medição de uma ou várias propriedades relevantes (de interesse).

How does one system simulate another?

Analog Quantum Simulator (AQS)

Quantum systems whose Hamiltonians can be engineered to map those of a subset of models put forward to describe a real system. The simulator mimics the continuous evolution of another system.

Digital Quantum Simulator (DQS)

The state of the simulated system is encoded using qubits, and its Hamiltonian discretized using Trotter decomposition to define which quantum gates to apply. [1]

How does one system simulate another?

Analog Quantum Simulator (AQS)

Quantum systems whose Hamiltonians can be engineered to map those of a subset of models put forward to describe a real system. The simulator mimics the continuous evolution of another system.

Digital Quantum Simulator (DQS)

The state of the simulated system is encoded using qubits, and its Hamiltonian discretized using Trotter decomposition to define which quantum gates to apply. [1]

Um AQS é um sistema cuja evolução (H) pode ser manipulada de forma a mapear, de acordo com um determinado modelo, a evolução de um sistema real (e por norma difícil de preparar, manipular e medir). Os AQS estão limitados ao conjunto de sistemas reais para os quais existe um mapeamento teoricamente correto. Um DQS decompõe (discretiza) o H, mapeando-o para um circuito, decompondo-se a sua evolução numa série de portas (gates) lógicas. Tal simulador pode eficientemente (em tempo polinomial) qualquer Hamiltoneano local de dimensão finita – um simulador quântico universal, que é equivalente a um computador quântico (neste caso, distinção entre um simulador quântico universal e um computador quântico está na função – estudar as propriedades físicas de um sistema vs realizar operações matemáticas abstratas.

Outline

Outline
1 Quantum Simulation
Motivation
Analog and digital quantum simulation
Assessing quantum simulators
2 Quantum Tomography
Quantum State Tomography
Quantum Process Tomography
3 Verifying high-complexity systems
Quantum interactive proofs
Blind quantum computation
4 Hands-on: IBM Q Network

O derradeiro objetivo é construir-se um DQS universal e poderoso, mas em termos de aplicações práticas e concretização, é a AQS que está mais ao alcance dos experimentalistas.

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;

Os simuladores quânticos, para terem interesse científico, devem satisfazer um conjunto de requerimentos. Não existe consenso sobre como definir formalmente esse conjunto, mas vários autores iniciaram esse caminho. Hauke por exemplo, especifica que um simulador quântico deverá ter: Relevância: os modelos simulados deverão possuir aplicações relevantes para a compreensão da mecânica quântica; Controlabilidade: dos seus parâmetros (a nível de inicialização, manipulação, evolução e deteção); Eficiência: o simulador deverá obter soluções de forma mais eficiente relativamente ao que é possível com um computador clássico: Fiabilidade: deverá ser possível confirmar que o comportamento do simulador corresponde de forma fidedigna à física do modelo ideal Como verificar que uma simulação ocorreu realmente da forma prevista? (DQS)

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;
- *Controllability*: the simulator should allow for broad control not only of the parameters of the simulated model, but preparation, manipulation and detection of the relevant observables;

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;
- *Controllability*: the simulator should allow for broad control not only of the parameters of the simulated model, but preparation, manipulation and detection of the relevant observables;

Os simuladores quânticos, para terem interesse científico, devem satisfazer um conjunto de requerimentos. Não existe consenso sobre como definir formalmente esse conjunto, mas vários autores iniciaram esse caminho. Hauke por exemplo, especifica que um simulador quântico deverá ter: Relevância: os modelos simulados deverão possuir aplicações relevantes para a compreensão da mecânica quântica; Controlabilidade: dos seus parâmetros (a nível de inicialização, manipulação, evolução e deteção); Eficiência: o simulador deverá obter soluções de forma mais eficiente relativamente ao que é possível com um computador clássico: Fiabilidade: deverá ser possível confirmar que o comportamento do simulador corresponde de forma fidedigna à física do modelo ideal Como verificar que uma simulação ocorreu realmente da forma prevista? (DQS)

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;
- *Controllability*: the simulator should allow for broad control not only of the parameters of the simulated model, but preparation, manipulation and detection of the relevant observables;
- *Efficiency*: it should solve problems more efficiently that what is practcally possible on a classical computer;

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;
- *Controllability*: the simulator should allow for broad control not only of the parameters of the simulated model, but preparation, manipulation and detection of the relevant observables;
- *Efficiency*: it should solve problems more efficiently that what is practcally possible on a classical computer;

Os simuladores quânticos, para terem interesse científico, devem satisfazer um conjunto de requerimentos. Não existe consenso sobre como definir formalmente esse conjunto, mas vários autores iniciaram esse caminho. Hauke por exemplo, especifica que um simulador quântico deverá ter: Relevância: os modelos simulados deverão possuir aplicações relevantes para a compreensão da mecânica quântica; Controlabilidade: dos seus parâmetros (a nível de inicialização, manipulação, evolução e deteção); Eficiência: o simulador deverá obter soluções de forma mais eficiente relativamente ao que é possível com um computador clássico: Fiabilidade: deverá ser possível confirmar que o comportamento do simulador corresponde de forma fidedigna à física do modelo ideal Como verificar que uma simulação ocorreu realmente da forma prevista? (DQS)

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;
- *Controllability*: the simulator should allow for broad control not only of the parameters of the simulated model, but preparation, manipulation and detection of the relevant observables;
- *Efficiency*: it should solve problems more efficiently that what is practcally possible on a classical computer;
- *Reliability*: one should be ensured that the observed physics of the QS corresponds faithfully to that of the ideal model;

Assessing quantum simulators

There is some progress [2][3] in devising a set of criteria which quantum simulators must fullfill. Hauke et. al. define such requirements:

- *Relevance*: the simulated models should be of relevance for applications in Quantum Mechanics;
- *Controllability*: the simulator should allow for broad control not only of the parameters of the simulated model, but preparation, manipulation and detection of the relevant observables;
- *Efficiency*: it should solve problems more efficiently that what is practcally possible on a classical computer;
- *Reliability*: one should be ensured that the observed physics of the QS corresponds faithfully to that of the ideal model;

Os simuladores quânticos, para terem interesse científico, devem satisfazer um conjunto de requerimentos. Não existe consenso sobre como definir formalmente esse conjunto, mas vários autores iniciaram esse caminho. Hauke por exemplo, especifica que um simulador quântico deverá ter: Relevância: os modelos simulados deverão possuir aplicações relevantes para a compreensão da mecânica quântica; Controlabilidade: dos seus parâmetros (a nível de inicialização, manipulação, evolução e deteção); Eficiência: o simulador deverá obter soluções de forma mais eficiente relativamente ao que é possível com um computador clássico: Fiabilidade: deverá ser possível confirmar que o comportamento do simulador corresponde de forma fidedigna à física do modelo ideal Como verificar que uma simulação ocorreu realmente da forma prevista? (DQS)

Outline

2018-03-16

Validação de Simulações Quânticas
└Quantum Tomography
 └Quantum State Tomography
  └Outline

Outline

1 Quantum Simulation
- Motivation
- Analog and digital quantum simulation
- Assessing quantum simulators

2 Quantum Tomography
- Quantum State Tomography
- Quantum Process Tomography

3 Verifying high-complexity systems
- Quantum interactive proofs
- Blind quantum computation

4 Hands-on: IBM Q Network

Quantum State Tomography

- Set of techniques for reconstruction of the quantum state from a source quantum system;
- The source must be able to consistently prepare the same state;
- The measurements must be tomographically complete - form an operator basis on the Hilbert space of the system.

Quantum State Tomography

- Set of techniques for reconstruction of the quantum state from a source quantum system;
- The source must be able to consistently prepare the same state;
- The measurements must be tomographically complete - form an operator basis on the Hilbert space of the system.

QUANTUM STATE TOMOGRAPHY é o nome de um conjunto de técnicas que permite a determinação e descrição completa do estado de um sistema quântico (ao contrário de uma simples medição, onde se observa apenas um outcome possível). Para tal é necessário que o sistema seja capaz de produzir o estado final várias vezes e de forma consistente, de modo a que este possa ser medido repetidamente através de um conjunto de operadores que forma uma base no espaço de Hilbert. Na sua formulação rigorosa e convencional, a tomografia de estados requer um número de operações (e de tempo) que escala exponencialmente com o tamanho do sistema.

Outline

Outline

1 Quantum Simulation
- Motivation
- Analog and digital quantum simulation
- Assessing quantum simulators

2 Quantum Tomography
- Quantum State Tomography
- Quantum Process Tomography

3 Verifying high-complexity systems
- Quantum interactive proofs
- Blind quantum computation

4 Hands-on: IBM Q Network

Quantum Process Tomography

- Reconstruct a *quantum process* using well defined quantum states;
- As with quantum state tomography, scales with the Hilbert space dimension.

Quantum Process Tomography

- Reconstruct a *quantum process* using well defined quantum states;
- As with quantum state tomography, scales with the Hilbert space dimension.

Similarmente, as técnicas de QUANTUM PROCESS TOMOGRAPHY utilizam estados quânticos bem definidos (por exemplo, utilizando quantum state tomography) para estudar e determinar um processo quântico desconhecido. Tal como acontece com a tomografia de estados, estas técnicas deverão escalar de acordo com o número de dimensões do espaço de Hilbert, que por definição aumenta exponencialmente com o número de qubits do sistema. [Vários autores propõem aproximações às técnicas de tomografia, que oferecem técnicas de escalamento polinomial desde que se relaxem as margens de erro aceitáveis na determinação do estado ou processo].

Outline

1. Quantum Simulation
   - Motivation
   - Analog and digital quantum simulation
   - Assessing quantum simulators
2. Quantum Tomography
   - Quantum State Tomography
   - Quantum Process Tomography
3. Verifying high-complexity systems
   - Quantum interactive proofs
   - Blind quantum computation
4. Hands-on: IBM Q Network

Outline
1. Quantum Simulation
- Motivation
- Analog and digital quantum simulation
- Assessing quantum simulators
2. Quantum Tomography
- Quantum State Tomography
- Quantum Process Tomography
3. Verifying high-complexity systems
- Quantum interactive proofs
- Blind quantum computation
4. Hands-on: IBM Q Network

Quantum interactive proofs

Aharonov and Vazirani [4] argue that the scientific paradigm of "predict and verify" cannot be applied to testing quantum mechanics in the limit of high complexity"

- How can a classical, computationally restricted experimentalist test the high complexity aspects of quantum mechanics?

Quantum interactive proofs

Aharonov and Vazirani [4] argue that the scientific paradigm of "predict and verify" cannot be applied to testing quantum mechanics in the limit of high complexity"

- How can a classical, computationally restricted experimentalist test the high complexity aspects of quantum mechanics?

Aharonov e Vazirani argumentam que o paradigma cientifico de "previsão e verificação" não pode ser aplicado ao estudo de sistemas quânticos nos limites de complexidade (i.e. a dimensão do espaço de Hilbert do sistema). Como poderá um experimentalista com poder de computação limitado testar sistemas quânticos tão complexos que não é possível computar uma previsão para o seu comportamento? É necessário estruturar o problema sob o prisma dos interactive proof systems:

Quantum interactive proofs

Quantum interactive proof system (QPIP)

Arthur, a computationally weak (i.e. polynomial strength) verifier, can interact with Merlin, a powerful, untrusted quantum system capable of performing quantum computations.

- Existing protocols [4] require Arthur to be able store, manipulate (at most) 3 qubits - the verifier needs to have at least some computational power.

Quantum interactive proofs

Quantum interactive proof system (QPIP)

Arthur, a computationally weak (i.e. polynomial strength) verifier, can interact with Merlin, a powerful, untrusted quantum system capable of performing quantum computations.

- Existing protocols [4] require Arthur to be able store, manipulate (at most) 3 qubits - the verifier needs to have at least some computational power.

Num quantum interactive proof system, um "provador" limitado computacionalmente (a tempo polinomial), Arthur, pode interagir com uma entidade muito mais poderosa, mas de fiabilidade duvidosa, Merlin. Neste contexto, Artur representa o experimentalista, e Merlin representa um sistema quântico onde é possível realizar operações quânticas. Apesar de Artur não poder verificar se o resultado de uma computação em particular estar correto, pode utilizar um protocolo que contrua uma sequência de experiências que em conjunto permitem testar a consistência da computação quântica. No entanto, os protocolEos existentes requerem que o verificador (Arthur) possua alguma capacidade de computação quântica: não deverá ser puramente clássico, mas poder armazenar e manipular até 3 qubits.

Quantum interactive proofs

Quantum interactive proof system (QPIP)

Arthur, a computationally weak (i.e. polynomial strength) verifier can interact with Merlin, a powerful, untrusted quantum system capable of performing quantum computations.

Theorem

$BQP \subseteq QPIP^*$

Quantum interactive proofs
Quantum interactive proof system (QPIP)
Arthur, a computationally weak (i.e. polynomial strength) verifier can interact with Merlin, a powerful, untrusted quantum system capable of performing quantum computations.
Theorem
BQP ⊆ QPIP*

Os autores provam [4] que este 'relaxamento' do quantum interactive proof, contém todos os problemas que podem ser eficientemente resolvidos por um computador quântico, ou seja [teorem]
Questão/objetivo: será que todos os problemas de computação quântica podem ser construídos como quantum interactive proof (em que o prover tem apenas computação clássica ao seu dispor?).

Outline

1. Quantum Simulation
   - Motivation
   - Analog and digital quantum simulation
   - Assessing quantum simulators
2. Quantum Tomography
   - Quantum State Tomography
   - Quantum Process Tomography
3. Verifying high-complexity systems
   - Quantum interactive proofs
   - Blind quantum computation
4. Hands-on: IBM Q Network

Outline

1. Quantum Simulation
   - Motivation
   - Analog and digital quantum simulation
   - Assessing quantum simulators
2. Quantum Tomography
   - Quantum State Tomography
   - Quantum Process Tomography
3. Verifying high-complexity systems
   - Quantum interactive proofs
   - Blind quantum computation
4. Hands-on: IBM Q Network

Blind quantum computation

- Different approach/motivation, similar techniques;
- Introduces the concept of blindness

Blind quantum computation

- Different approach/motivation, similar techniques;
- Introduces the concept of blindness

Hands-on: IBM Q Network

- Goal: apply some of the described protocols to the quantum language developed by IBM for its quantum computers;

Hands-on: IBM Q Network

- Goal: apply some of the described protocols to the quantum language developed by IBM for its quantum computers;

Summary

└─Summary

For Further Reading I

Lloyd, S.
Universal Quantum Simulators.
Science, (1996): 1073-1078.

Cirac, J. Ignacio, Zoller, P.
Goals and opportunities in quantum simulation.
Nature Physics 8.4 (2012): 264.

Hauke, P. et al.
Can one trust quantum simulators?
Reports on Progress in Physics, 75.8: (2012): 082401.

Aharonov, D., Vazirani, U.
Is Quantum Mechanics Falsifiable? A computational perspective on the foundations of Quantum Mechanics
Computability: Turing, Gödel, Church, and Beyond. MIT Press, 2013.

For Further Reading I

Lloyd, S.
Universal Quantum Simulators.
Science, (1996): 1073-1078.

Cirac, J. Ignacio, Zoller, P.
Goals and opportunities in quantum simulation.
Nature Physics 8.4 (2012): 264.

Hauke, P. et al.
Can one trust quantum simulators?
Reports on Progress in Physics, 75.8: (2012): 082401.

Aharonov, D., Vazirani, U.
Is Quantum Mechanics Falsifiable? A computational perspective on the foundations of Quantum Mechanics
Computability: Turing, Gödel, Church, and Beyond. MIT Press, 2013.